UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,350	07/20/2000	William J Reid	AUS990912US1	3424

35525 7590 05/24/2004

DUKE W. YEE
CARSTENS, YEE & CAHOON, L.L.P.
P.O. BOX 802334
DALLAS, TX 75380

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/620,350	REID, WILLIAM J	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. The Amendment of February 2nd, 2004 has been received and entered.

2. In light of the amendments made, the rejections to claims 4, 5, 15, 16, 25, 26, 29 under 35 USC 112 second paragraph are withdrawn.

Response to Arguments

3. Applicant's arguments filed February 2nd, 2004 have been fully considered but they are not persuasive.

Applicant argues on Page 14, Paragraph 1:

"Glasser does not disclose changing security information in a centralized server. Instead Glasser generally discloses changing security information for a particular server at the server. For example in Col 7, Lines 46-48, Glasser states that when changing access permission to a resource controlled by peer server 120, "commands for manipulating resource access permissions are assumed to be received from user interface 125 of peer server 120". Thus security information is not changed in a centralized server but is changed at server 120 itself via GUI 125 associated with the server.

Although as pointed out by Examiner, the commands can also come from a remote source or from another node of the network (col. 7, lines 48-54 of Glasser), the change in access information for the resource stored in hard disk 121 is still being made in peer server 120 and not from a centralized server."

The Examiner maintains that Glasser changes security information in a centralized server. The server which must inherently serve clients. From this sense, the server is centralized in that it is the central point from which the clients access a given type of information. Because the clients are accessing resources from the server, from the clients' perspective, the server is centralized connection point to the other clients.

Furthermore, the Examiner maintains that information that is changed at the server itself via GUI associated would not change whether a server was centralized or not. In fact, because a server by definition serves clients, the information in any server whether centralized or not, would have to at some point be changed at the server itself since it is from the server from which the client accesses the resources. Whether the command to manipulate is the resource access permissions is received from the user interface or from other network nodes are considered irrelevant since the final result of the update command would still be a change in the access permissions of the server.

Applicant additionally argues on page 14 paragraph 3:

"Glasser also does not disclose downloading changed security information to a plurality of servers in response to an update command. Again, in Glasser, security information appears to be downloaded to a resource associated with a particular server from that particular server, not a plurality of server in response to an update command.

During the above mentioned interview the Examiner pointed out that files stored on hard disk 121 associated with peer server 120 are arranged in a hierarchical manner, and that Glasser could, perhaps, be construed as reading on claim 1 by virtue of changing security information being downloaded through the hierarchy.

Applicant respectfully disagrees."

Applicant then rebuts on page 16, paragraph 1:

"In Glasser, peer server 120 receives a command to change the permissions for a selected resource. Peer server 120 then determines if the resource, e.g. a particular folder, has its own ACL. If so, the folder's own ACL is updated. If not, the nearest ancestor having an ACL is determined, and that ACL is updated.

Thus even if the files and folders stored in hard disk 121 can be considered as being "servers", which Applicant does not believe to be the case, security information is still being changed only in a particular ACL for a folder or file, and changed security information is not downloaded from a centralized server to a plurality of servers in response to receiving an update command as recited in claim 1."

The Examiner maintains that a server and client are relative terms in the art and is a purely conceptual construction. A server then is deemed a server because of its function and what it does.

For example Glasser (Column 1, lines 30-45) indicate that

"If a user of computer B wishes to access a file stored remotely on the disk of computer A, then computer B is the client and computer A is the server."

"If the user of computer A wishes to print a locally stored file using the printer of computer B, then computer A becomes the client and computer B is the server."

Glasser describes a server computer as such:

"In a network, a server computer is one that provides a resource to a client computer. The same computer can be client in one context and server in another."

Thus, the aspect of the server computer that makes it a "server" lies within the ability to provide a resource or resources to clients. The Examiner maintains then that the file and folder system as disclosed by Glasser (Figure 9), can indeed be construed as servers since it is from the folders from which a client may access a particular resource such as files. Additionally, the folders themselves are even disclosed to contain individual access control lists. Thus each folder is also individual point of authentication and authorization, further implying each folder as a separate conceptual entity.

In regards to applicant's arguments in which state:

"security information is still being changed only in a particular ACL for a folder or file, and changed security information is not downloaded from a centralized server to a plurality of servers in response to receiving an update command as recited in claim 1."

The sections of Glasser cited for Claim 1 previously, recites:

"Commands for manipulating resource access permissions are assumed to be a received from a user interface of peer server 120. It will be appreciated that the commands could also come from other sources, such as a script executed by processor 122 or, in some circumstances from another node of the network."

"Peer server 120 receives a command to change the permissions for the selected resource(step B). If the command is null, so that there are no changes to be made(step C), the remaining steps of figure 5 are skipped. Otherwise, peer server 120 alters the resource access permissions responsively to the received command(Step D), propagates changes to the descendants of the resource in the hierarchy"

Because a command to manipulate a resource access permission or an "update command received" results in the changes being propagated to the descendants of the resource in the hierarchy, and these resources are understood by applicant as folders and files, the Examiner maintains that security information is indeed downloaded from a centralized server to a plurality of servers in response to receiving an update command as recited in claim 1.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35, 37-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Glasser et al.

In reference to claim 1:

Glasser et al. discloses a method of updating security configurations of a plurality of servers, comprising:

- Changing security information in a centralized server, where the security information is the commands for manipulating resource access permissions (Column 7, lines 45-48)
- Receiving an update command (Column 7, lines 46-48)

- Downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers, where the downloaded information occurs when the security information is propagated down the network. (Column 7, lines 60-65)

In reference to claim 2:

Glasser et al. discloses a method wherein the plurality of servers are Windows NT servers and the centralized server is a directory server. (Column 3, lines 34-40)

In reference to claim 3:

Glasser et al. discloses a method wherein the centralized server is a directory server and wherein changing the security information includes using an editor to change a directory listing in the centralized server, where the editor is the program that allows the security information to be changed. (Column 8, lines 12-39)

In reference to claim 4:

Glasser et al. discloses a method where the security configurations of the plurality of servers are updated by updating security parameter lists associated with a plurality of files and resources associated with each of the plurality of servers, where the security configurations are altered through the access control list and each list is associated with a plurality of files and resources for its particular node in the network (Column 9, lines 15-25)

In reference to claim 5:

Glasser et al. discloses a method where the security parameter lists identify authorized users or authorized groups of users of the files and resources associated with the security parameter lists, where the security parameter lists are access control lists which identify authorized groups of users of the files and resources. (Column 7, lines 5-12)

In reference to claim 6:

Glasser et al. discloses a method where the update command is received from a network administrator, where the network administrator is the system administrator (Column 7, lines 46-54)

In reference to claim 8:

Glasser et al. discloses a method where the update command is received from one or more of the plurality of servers, where the update command is the request for changing resource access permissions, and the plurality of servers is any node on the network (Column 7, lines 46-54)

In reference to claim 10:

Glasser et al. discloses a method where downloading the changed security information includes filtering a directory listing stored on the centralized server to extract the changed security information, where the directory listing is filtered and only the changes made with respect to the selected resources are propagated to the rest of the nodes. (Column 9, lines 15-25)

In reference to claim 11:

Glasser et al. discloses a method where the security configurations are updated by filtering the downloaded changed security information to extract only necessary update information for updating the security configurations and then updating the security configurations based on the extracted necessary update information, where the security configurations are updated by filtering the changes and updating only the changes. (Column 7, lines 55-64)

In reference to claim 14:

Glasser et al. discloses a security configuration update server wherein the update command includes changes to the security information. (Column 8, lines 47-54)

In reference to claim 32:

Glasser et al. discloses a method in a data processing system for updating access information for a plurality of servers, the method comprising:

Collecting changes to access information at the data processing system to form modified access information and responsive to a policy, transferring the modified access information to the plurality of servers, wherein the modified access information is used to update the security configurations of the plurality of servers. (Column 9, lines 15-25)

In reference to claim 33:

Glasser et al. discloses a method wherein the policy comprises receiving a request to update the security configurations for the plurality of servers. (Column 7, lines 46-48)

In reference to claim 35:

Glasser et al. discloses a method wherein the policy comprises initiating the transfer of the modified access information to the plurality of servers in response to a selected event, where the selected event is the received command for manipulating access information. (Column 7, lines 46-48) & (Column 8, lines 35-39)

In reference to claim 40:

Glasser et al. discloses a method wherein the security information is filtered by the centralized server, prior to downloading the security information, to extract only security information that has been changed, where the server filters the information before downloading the security information and the information is only sent if changes made with respect to the selected resource can be propagated. (Column 9, lines 15-20)

Claims 12, 23, 37 are rejected for the same reasons as claim 1.

Claims 13, 38 are rejected for the same reasons as claim 2.

Claim 24 is rejected for the same reasons as claim 3.

Claims 15, 25, 39 are rejected for the same reasons as claim 4.

Claims 16, 26 are rejected for the same reasons as claim 5.

Claims 17, 27 are rejected for the same reasons as claim 6.

Claims 19, 29 are rejected for the same reasons as claim 8.

Claims 21, 31 are rejected for the same reasons as claim 10.

Claim 22 is rejected for the same reasons as claim 11.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 7, 9, 18, 20, 28, 30, 34, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Glasser et al.

In reference to claim 7:

Glasser et al. discloses all of claim 7 except a method wherein the update command is received at scheduled periodic times.

The examiner takes official notice that receiving the update command at scheduled periodic times is well known to those of ordinary skill in the art. For example, System or network administrators often do routine maintenance based on a schedule.

It would have been obvious to one of ordinary skill in the art for an administrator to send out an update command, and hence have an update command received at scheduled periodic

times, because it would allow clients of the system to know when to expect an access control update, should the update temporarily interfere with their own ability to access the server while the access control list was being updated.

In reference to claim 9:

Glasser et al. discloses all of claim 9 except a method wherein the centralized server is a light weight directory access protocol server.

The examiner takes official notice that the lightweight directory access protocol, or LDAP is well known to those of ordinary skill in the art. LDAP defines a standard manner of organizing directory hierarchies and a standard interface for clients to interface with access directory servers.

It would have been obvious to one of ordinary skill in the art to use the lightweight directory access protocol in the central server because LDAP has broad industry support, and runs directly over TCP/IP.

Claims 18, 28, 34, 36 are rejected for the same reasons as claim 7.

Claims 20, 30 are rejected for the same reasons as claim 9.

Conclusion

8. The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US Patent 5335346 discloses a an access control list which spans the boundaries of objects. Access control policies are implemented from an object's superobject.
- US Patent 5173939 discloses a distributed system where each object in the system contains its own Access Control List. These objects are connected to a Trusted Computing Base
- US Patent 5701458 discloses ACLs associated with each directory, file, printer, or other resource in a data processing system with a hierarchical structure.

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

May 17th 2003

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137